FEDERAL PKI POLICY AUTHORITY

December 11, 2012 MEETING MINUTES

GSA NOMA
One Constitution Square
Conference Room 401
1275 1st Street, NE,
Washington, DC 20417
9:30 a.m. – 12:00 p.m. EST

9:30	**Welcome, Opening Remarks & Introductions**	**Deb Gallagher, Chair**
9:35	**Discussion/Vote: November 2012 FPKIPA Minutes**	**Matt King**
9:45	**FPKIPA Chair Update**	**Deb Gallagher**
10:05	**FPKI Management Authority (FPKIMA) Report**	**Darlene Gore**
10:25	**FPKI Certificate Policy Working Group (CPWG) Report** **1. Status: PIV Content Signing Policy Change Proposal (Common CP)** **2. Mapping Updates** **3. Other Updates**	**Charles Froehlich**
10:45	**SHA-1 Transition Status**	**SHA-1 Affiliates**
10:50	**Adjourn Meeting**	**Deb Gallagher**
10:51	**Holiday Celebration**	**All**

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Bures, Iva	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	T
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Paul	P
Department of Treasury (Treasury)	Wood, Dan	P
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	A
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	Proxy to GSA
Veterans Administration (VA)	Jurasas, Eric	T

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
IdenTrust	Cox, Jerry	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
FPKIPA (Contractor, Protiviti)	King, Matt	T
FPKIPA (Contractor, Protiviti)	Louden, Chris	P
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
FPKIMA (Contractor, Protiviti)	Brown, Wendy	P
SAFE	Wilson, Gary	T
ProTegus, LLC	Shomo, Larry	T

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at GSA NOMA, One Constitution Square, Conference Room 401, 1275 1st Street, NE, Washington, DC 20417. Ms. Deb Gallagher, Chair, called the meeting to order at 9:30 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on November 6, 2012 FPKIPA Minutes, Matt King

There was a vote to approve the November 6, 2012 FPKIPA minutes. GSA motioned to approve; NRC seconded. The motion was approved unanimously.

Approval Vote for November 6, 2012 FPKIPA Minutes			
Voting members	**Vote (GSA Motion; NRC Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ) – Proxy to GSA	√		
Department of State (State) – Proxy to GSA	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)			Absent
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)			Absent
Nuclear Regulatory Commission (NRC)	√		
Social Security Administration (SSA)	√		Absent
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

FPKIPA Chair Update, Deb Gallagher

Ms. Gallagher presented the FPKIPA Chair Report. Upcoming meetings and events include:

ISIMSC	December 12, 2012
Mobile Technology Tiger Team (bi-weekly)	December 13, 2012
Federal Mobile Security Conference/Technical Exchange Meeting	December 14, 2012 (Gaithersburg)
CPWG	December 18, 2012
ICAMSC	January 30, 2013
IAB	January 30, 2013

Ms. Gallagher provided an overview of current working group activities. Discussions were held at the Federal Mobile Security conference about the mobile tiger team and mobile efforts across the Government. There is an effort in the ACAGWG to coordinate IdM across various fabrics. There is also a need and effort to align guidance for PKI in secret and federal fabrics. Ms. Gallagher presented the *PIV-I for Non-US Persons* concept to the ICAMSC and it was well-received. Ms. Judy Spencer also mentioned a new FAA rule requiring all pilots flying in or out of the U.S. to have FIPS 201 compliant credentials.

The next FPKIPA meeting is January 15, 2013. The meeting will be at GSA.

FPKIPA Chair Report_11DEC12.ppt

FPKI Management Authority Report, Darlene Gore

Ms. Wendy Brown presented the FPKIMA Report. The FPKIMA observed a cyber security exercise at the *National Cybersecurity and Communications Integration Center* (NCCIC). The FPKIMA will present a PKI 101 briefing for the NCCIC and assist them in planning an exercise related to PKI CAs. Updates on recent certificate issuances, TWG efforts, recent network updates and FPKI repository performance were provided in the briefing below. Mr. Tim Baldridge commented that the improvements to FPKI operations and processes in the last several years have been nothing short of a miracle.

Ms. Brown noted that the Common Policy Root is included in the following Root stores: Microsoft, Adobe, and Apple. The FPKIMA is still working to get the Common Policy Root included in Mozilla and Opera, and is investigating how to get it included in Java.

Dec2012 Slides for PA Meeting - final.pdf

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. Discussion/Vote: PIV Content Signing Policy Change Proposal

The CPWG discussed this change proposal in terms of identifying concerns or objections to the proposal. It was noted that SSA had raised an objection to the requirement to implement the new policy OID within a year of FIPS 201-2 being signed. The CPWG determined that the proposal, as currently written, did not mandate implementation to the exclusion of existing techniques. With NIST participation, it was determined that NIST would incorporate an implementation date into FIPS 201-2 (expected to be in 2nd quarter, CY 2015).

The objection to including physical security and access control requirements for PKI card issuance systems was also discussed with NIST. DoS proposed adding these requirements into either FIPS 201 or NIST SP 800-79. NIST noted that FIPS 201 was probably not appropriate and it was too late to introduce additional changes. However, NIST SP 800-79 is coming due for review and such requirements could be incorporated there or into NIST SP 800-53.

b. Mapping Updates

VeriSign (Symantec) was a modified mapping review to satisfy the Symantec request for cross-certification at Medium-HW. A full baseline mapping will be conducted at a later date once Symantec enters the queue. Some questions were identified and have been sent back for clarification.

IdenTrust policy mapping has begun (completed 4 of 10 sections). Some questions were identified and have been sent back for clarification.

After using the new baseline policy mappings, the CPWG has identified a number of instances in which the FBCA and/or FCPCA need to be updated to eliminate outdated language. We are compiling a list of those instances for review and modification.

Follow-On Actions:
DoD mapping is completed with two exceptions: (1) addition of SHA-2 OIDs, and (2) two policy mapping changes that are FBCA CP requirements remain unresolved and may require specific approval by the FPKIPA. White space mapping, operational

parameters, and profile review remain to be completed. Auditing is completed. Operational testing is not necessary.

ExoStar mapping and requested updates are completed. White space mapping, operational parameters, and profile review remain to be completed. Zero-day audit and operational testing to be conducted in late January 2013. An MOA is being drafted.

USPS mapping is completed. White space mapping, operational parameters, and profile review remain to be completed. Operational testing is completed and a report is pending. An MOA draft is pending.

c. Other Updates

DoD ECA Cross-Certification Application: The DoD submitted their application and the architecture diagram will be reviewed at the December 18, 2012 CPWG meeting.

Review of the *Digital Signature Change Proposals* continues. These proposals were held over due to some concerns about the validity of digital signatures in archive records and the lack of a federal policy to establish the capability. It was suggested that additional language be included to the effect that, "The FPKIPA recognizes that the Federal Government has not established policy regarding long term validation of digital signatures. Lack of such policy may affect the ability to validate PKI archive records. Since PKI records are archived for up to 20 years and six months, Federal guidelines need to be written." Mr. Larry Shomo will provide additional language to be incorporated in the CP archival sections. Ms. Spencer mentioned that it might be beneficial to coordinate with NARA on such a policy.

The CPWG is forming a Tiger Team to relook at the mapping tables to eliminate some of the perceived duplication and confusion. If anyone wishes to participate, please inform the CPWG Chair as soon as possible.

SHA-1 Transition Status, SHA-1 Affiliates

As of November 28, 2012, NRC has stopped issuing SHA-1 certificates under the Common Policy. Illinois is moving to SHA-2 as well. CertiPath is planning its transition to SHA-2 but it requires close coordination with DoD since maintaining interoperability between DoD and the rest of the Federal Government is critical. The DoD schedule for transitioning to SHA-2 is expected to be released in early 2013. SAFE is standing up a SHA-2 CA in Q1 of 2013.

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 10:47 a.m. EST.

FPKIMA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	12-Jul-11	13-Sep-11	Open
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSs	Wendy Brown	8-May-12	30-Jul-12	Open
464	Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.	Darlene Gore, Jeff Jarboe	10-Jul-12	17-Jul-12	Closed
466	Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.	Deb Gallagher	10-Jul-12	17-Jul-12	Closed
467	Mr. Slusher will draft language with Mr. Froehlich, Mr. King, and Mr. Silver, to add language about PKI uses and business processes to the FPKI Criticality letter and send the final version to Ms. Gallagher.	Toby Slusher	14-Aug-12	11-Sep-12	Closed
468	Ms. Gallagher will submit the final FPKI Criticality Letter to the ICAMSC.	Deb Gallagher	14-Aug-12	30-Sep-12	Closed
469	The FPKIMA will send information to the FPKIPA mail list about how to participate in the Mozilla discussion.	Wendy Brown	14-Aug-12	11-Sep-12	Closed
470	Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents	Charles Froehlich	14-Aug-12	11-Sep-12	Open
471	The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA	Charles Froehlich	14-Aug-12	11-Sep-12	Open
472	Mr. Froehlich will lead discussions in the CPWG to develop a PIV Content Signing change proposal.	Charles Froehlich	14-Aug-12	11-Sep-12	Closed

Number	Action Statement	POC	Start Date	Target Date	Status
473	Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.	FPKI Affiliates	14-Aug-12	11-Sep-12	Open
474	Mr. Jason Miller will work to obtain more detailed information on the VA remediation efforts.	Jason Miller	14-Aug-12	11-Sep-12	Closed
475	Ms. Gallagher will resubmit the metrics related to the FPKI Security Profile to the FISMA team	Deb Gallagher	14-Aug-12	11-Sep-12	Closed